UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. HERBERT REDHOLTZ, Defendants.	Case No. 2:22-cr-00433-MCS-1 **ORDER DENYING DEFENDANT'S MOTIONS TO SUPPRESS (ECF NOS. 56, 57)**

Defendant Herbert Redholtz moves to suppress "all digital evidence," (Mot. 1, ECF No. 56), and all evidence "obtained as a result of the warrantless search in this case," (Mot. 2, ECF No. 57). The Government opposed both motions, (Opp'n, ECF No. 61), and Defendant replied, (Reply 1, ECF No. 64; Reply 2, ECF No. 65). The Court heard argument on March 4, 2024. The Court deferred ruling on the motions until it received additional information by way of a status report or stipulation. (Mins., ECF No. 69.) On March 22, 2024, Defendant filed a status report, (Def. Status Report, ECF No. 73), and the Government filed a status report, (Gov. Status Report, ECF No. 72). Additionally, the Government filed a response to Defendant's status report. (Gov. Resp., ECF No. 74.)

I. BACKGROUND

According to a Department of Homeland Security investigation report, on October 17, 2014, Defendant attempted to send an email from his Microsoft email account that contained a suspected child pornography image. (Mot. 1 Ex. G, ECF No. 56-2.) Microsoft reported the email to the National Center for Missing and Exploited Children ("NCMEC") using a technology called PhotoDNA. (Mot. 2 Ex. B, ECF No. 57-2) NCMEC generated a CyberTip report (also referred to as a "NCMEC report") for the flagged email and shared the CyberTip report with the Department of Homeland Security, Homeland Security Investigations organization ("HSI") in Los Angeles. (*Id*.) The case was assigned to HSI Special Agent Kimmesia Sampson. (Mot. 1 Ex. G.)

In January 2015, Agent Sampson sent an order to Microsoft directing it to produce requested connection logs and records for Defendant's email pursuant to 18 U.S.C. § 2703(d). (Mot. 1 Ex. A, at USAO_000304–05.) On March 12, 2015, Microsoft transmitted data responsive to the § 2703(d) order. (Sampson Decl. Ex. B, ECF No. 72-2.) On March 17, 2015, a search warrant was issued for Defendant's email, which was served on Microsoft that same day. The 2015 warrant permitted the search team to "complete its search of the content records as soon as is practicable but not to exceed 60 days from the date of receipt from the PROVIDER of the responses to this warrant." (Mot. 1 Ex. A at USAO_000314.) On March 19, 2015, Microsoft sent a transmittal notice to HSI. (Mot. 1 Ex. C.) On May 21 or 22, 2015, Microsoft produced the email search warrant data ("Microsoft data" or "email data"). (Cushing Decl. Ex. B, ECF No. 72-1; Mot. 1 Ex. D, at USAO_000360; Sampson Decl. Exs. A, D–E.)[1]

On June 8, 2015, the Government obtained a warrant to search Defendant's

---

[1] In its status report, the Government provided evidence that Microsoft produced this evidence on either May 21 or 22, 2015. Because there are no allegations Agent Sampson reviewed the Microsoft data between July 20 and 21, 2015, the two possible dates by which the Government was required to conclude its search of the Microsoft data, the Court need not resolve this discrepancy.

home. (Mot. 1 Ex. H.) Similar to the search warrant issued for Defendant's email, the June 2015 warrant required the search team to complete the search of the digital devices located in Defendant's home within 60 days of their seizure or to request an extension. (*Id.* at USAO_000383.) On June 16, 2015, law enforcement searched Defendant's home and seized two digital devices. (Mot. 1 Ex. I.) On August 5, 2015, Defendant requested that the devices be returned to him. (Mot. 1 Ex. J.) Law enforcement denied Defendant's request for relief. (*Id.*) The Government proffers, and Defendant does not contest, that the forfeiture was complete in January 2016. (Opp'n 8–9; Reply 1 at 9 n.4.)

According to the Government, Agent Sampson left the Los Angeles HSI office, and the case was reassigned to HSI Special Agent Derek Baker in November 2019. (Opp'n 5–6.) Prior to leaving HSI, Agent Sampson did not complete her review of the email data from Microsoft, nor had she documented any progress regarding her review of the physical devices. (Mot. 1 Ex. D, at USAO_000362.) On June 3, 2020, Agent Baker filed an affidavit in support of an application for a new warrant to review the Microsoft data and the digital devices. (*Id.* at USAO_000362–63.) The 2020 warrant was issued on June 3, 2020, and authorized Agent Baker to review the physical devices and the Microsoft data without a date limitation. (*Id.* at USA_000344–53.) According to the Government, Agent Baker then reviewed the email data produced in 2015 as well as the digital devices. (Opp'n 8–9.) The Government's case is "based exclusively on Agent Baker's review and seizure of the content of defendant's email pursuant to the 2020 warrant," in which Agent Baker purportedly identified hundreds of images and videos as child pornography. (*Id.* at 8.)

II. LEGAL STANDARD

The Fourth Amendment provides in relevant part that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. "The Fourth Amendment does not proscribe all state-initiated searches and seizures; it merely proscribes those which are unreasonable." *Florida v. Jimeno*, 500 U.S. 248, 250 (1991); *accord Morgan*

v. United States, 323 F.3d 776, 780–81 (9th Cir. 2003) (quoting *id.*). Generally, "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)).

The exclusionary rule "often requires trial courts to exclude unlawfully seized evidence in a criminal trial." *Utah v. Strieff*, 579 U.S. 232, 237 (2016). "[T]he exclusionary rule encompasses both the primary evidence obtained as a direct result of an illegal search or seizure and . . . evidence later discovered and found to be derivative of an illegality, the so-called fruit of the poisonous tree." *Id.* (internal quotation marks omitted). But "the significant costs of this rule have led [the Supreme Court] to deem it applicable only . . . where its deterrence benefits outweigh its substantial social costs. *Id.* (ellipsis in original) (internal quotation marks omitted). Moreover, "the exclusionary rule does not apply when the police conduct a search in objectively reasonable reliance on a warrant later held invalid," nor when a police officer conducts a search "in objectively reasonable reliance on binding judicial precedent." *Davis v. United States*, 564 U.S. 229, 238–39 (2011) (internal quotation marks omitted). The Supreme Court has "never applied the exclusionary rule to suppress evidence obtained as a result of nonculpable, innocent police conduct." *Id.* at 240 (internal quotation marks omitted).

III. DISCUSSION

Defendant argues that all evidence derived from the Government's search of his Microsoft email account and digital devices must be suppressed because: Agent Sampson's initial search of the email and image from the NCMEC report was unconstitutional; the majority of content from the email data searched by Agent Sampson predated the date rage specified in the 2015 warrant; the HSI search team searched the email data outside the 60-day window permitted in the 2015 warrant; the Government unreasonably delayed in applying for the 2020 warrant to search the email data and digital devices; and the 2020 warrant to search the email data and digital

devices was overbroad and insufficiently particular. (*See generally* Mot. 1; Mot. 2.)

A. 2015 Warrant

1. Motion 2

Defendant argues Agent Sampson exceeded the scope of Microsoft's private search of the October 17, 2014 image that generated the original NCMEC report when she opened the email and photograph attached to the report. (Mot. 2, at 5–9.) Therefore, he argues, the Court should suppress "all evidence obtained as a result of the warrantless search in this case" because Agent Sampson's search exceeded the scope of the private search exception. (*Id.* at 9.) The Government counters that Agent Sampson's opening and viewing of the email and image attached to the NCMEC report, prior to receiving a warrant, was objectively reasonable based on binding judicial precedent at that time and therefore should not be excluded. (Opp'n 15–17); *see Davis*, 564 U.S. at 239.

The private-search exception to the exclusionary rule "concerns circumstances in which a private party's intrusions would have constituted a search had the government conducted it and the material discovered by the private party then comes into the government's possession." *United States v. Wilson*, 13 F. 4th 961, 967 (9th Cir. 2021). Under this exception, the government may warrantlessly view records produced by private parties so long as "the government search does not exceed the scope of the private one." *Id.* at 968.

At the time Agent Sampson opened and viewed the email and image attached to the NCMEC report, the controlling authority on the private search exception was *United States v. Tosti*, 733 F.3d 816 (9th Cir. 2013). In *Tosti*, the defendant took his computer to a repair shop where the technician opened a folder containing thumbnail images. *Id.* at 818–19. It was clear to the technician that the thumbnail images depicted child pornography. *Id.* at 819. The technician called the police, who viewed the thumbnail images, then directed the technician to enlarge the thumbnail images and place them into a slide deck so the officers could scroll through the images again. *Id.* The Ninth Circuit found the officers' actions did not exceed the scope of the private search

exception but, even if they had, suppression of this evidence was not warranted when the government did not learn any new information from an expanded search. *Id.* at 822. So too here.

At the time Agent Sampson reviewed the NCMEC report, she was able to assess that it included a PhotoDNA match from Microsoft that contained suspected child pornography. (*See* Mot. 2 Ex. B.) As explained by Agent Sampson in her affidavit supporting the 2015 warrant, PhotoDNA is "a technology developed by Microsoft that computes the hash values of images in order to identify alike images." (Mot. 2 Ex. D, at USAO_000394 n.2.) A "hash value" is an identifier for digital data, such as a photograph. (*Id.* at USAO_000394.) When a hash value is obtained for an image, another identical image will have the same hash value. (*Id.*) If the data on the image is changed, even slightly, the hash value will change. (*Id.*) Thus, "if two images have the same hash value, there is an extremely high likelihood that the images are the same." (*Id.*)

Therefore, prior to reviewing the email and image attached to the NCMEC report, Agent Sampson already knew Microsoft used PhotoDNA to compare the hash values of the attached image to hash values maintained by NCMEC, and that this comparison yielded a match for child pornography. (Mot. 2 Ex. D, at USAO_000394–95.) By opening the attached email and image, Agent Sampson learned no new information—just further confirmation of what Microsoft had already relayed—that PhotoDNA identified the image as child pornography. Thus, Agent Sampson's review of the attachments to the NCMEC report did not exceed the scope of the private search. *See Tosti*, 733 F.3d at 822.

Even if Agent Sampson's actions exceeded the scope of the exception, she acted with the reasonable, good-faith belief that her conduct was lawful based on *Tosti*. *See Davis,* 564 U.S. at 241 ("Evidence obtained during a search conducted in reasonable reliance on binding precedent is not subject to the exclusionary rule."). It was objectively reasonable for Agent Sampson to believe she would glean no new

information from reviewing the attachments to the NCMEC report since she already knew the hash value of the attached image had the same "digital DNA" as an image of child pornography maintained in NCMEC's database. (Mot. 2 Ex. D, at USAO_000394–95); *see Tosti*, 733 F.3d at 822. Therefore, evidence derived from Agent Sampson's initial review of the image and attachment to the NCMEC report need not be suppressed. *See United States v. Coyne*, 387 F. Supp. 3d 387, 402 (D. Vt. 2018) (declining to exclude evidence despite government's violation of the private search exception and noting that "[s]earches conducted on the good faith belief that no warrant was necessary are subject to the exception"). Defendant's second motion to suppress is denied.

2. Motion 1

Defendant argues that all evidence derived from Agent Sampson's search of his Microsoft data must be suppressed because the majority of content from the email data searched by Agent Sampson predated the date range specified in the 2015 warrant and, separately, because Agent Sampson searched the email data outside the 60-day window permitted in the 2015 warrant. (Mot. 1, at 4–8, 13.)

It is undisputed that in response to the 2015 warrant, Microsoft produced data beyond the date limitation set forth in the warrant. (Mot. 1, at 5–6; Opp'n 18; *see also* Mot. 1 Ex. A, at USAO_000292 (requiring disclosure of all emails and communications from Defendant's email account on "on or after October 17, 2014").) However, Microsoft's overproduction does not constitute a Fourth Amendment violation in itself. *See Wilson*, 13 F.4th at 967 ("[T]he Fourth Amendment protects individuals from government actors, not private ones . . . ."). As the Government persuasively notes, the 2015 warrant did not limit the Government from searching all records Microsoft turned over in response to the warrant in the event of an overproduction. (Opp'n 18 (citing Mot. 1 Ex. A, at USAO_000290–92).) Therefore, Agent Sampson did not exceed the scope of the warrant by reviewing documents preceding October 17, 2014.

Defendant avers Microsoft produced responses to the warrant on March 19, 2015,

meaning the Government had to conclude its search by May 18, 2015. (Mot. 1, at 6–7.) The Government argues that Microsoft produced responses to the § 2703(d) order in March 2015, but did not produce responses to the warrant until either May 21 or 22, 2015. (Opp'n 5; Cushing Decl. Ex. B; Mot. 1 Ex. D, at USAO_000360; Sampson Decl. Exs. A, D–E.) Thus, it argues, the search did not need to be concluded until July 20 or 21, 2015. (*Id.*)

The Court disagrees with Defendant that there remains a live factual dispute as to when Microsoft produced documents responsive to the warrant. (Def. Status Report 2.) On March 12, 2015, prior to service of the 2015 warrant, Microsoft produced documents to the Government. (Cushing Decl. Ex. A; Sampson Decl. Exs. B–C.) On March 19, 2015, Microsoft sent a transmittal notice to law enforcement. (Mot. 1 Ex. C.) Although the notice reads that "[Microsoft has] enclosed responsive documents," there is no other context for the notice nor evidence in the record that Microsoft actually sent any documents to the Government on this date. (*See id.*) In fact, the Government represents that this "data did not contain any content for the emails." (Opp'n 4.) Defendant argues it is more reasonable to assume Microsoft produced documents responsive to the 2015 warrant just two days after Microsoft received the warrant. (Def. Status Report 5 ("March 19, 2015 also makes logical sense as Microsoft's production date, since it was just two days after Microsoft received the warrant and occurred during the 10-day time period within which Microsoft was ordered by the warrant to provide the requested information.").) Defendant makes this argument fully aware that it took Microsoft roughly two months to produce records responsive to the § 7203(d) order. (*See* Mot. 1 Ex. A, at USAO_000304–05; Cushing Decl. Ex. A; Sampson Decl. Exs. B–C.) Defendant also makes this argument fully aware that Microsoft ultimately produced 618,966 files that spanned roughly seven years. (Gibson Decl. ¶¶ 5–10, ECF No. 56-1.) The notion that Microsoft was capable of searching for and then producing such a massive production just two days after receiving a warrant, even though it required nearly two months to produce documents responsive to the § 7203(d) order, is

implausible. Moreover, Defendant provided no evidence to support its position aside from the innocuous March 19, 2015 transmittal notice and no argument as to what Microsoft's voluminous May 2015 production might be if not responsive to the warrant.

Therefore, the Court finds that the Government's deadline to review the Microsoft data pursuant to the 2015 warrant was either July 20 or 21, 2015,[2] 60 days after Microsoft produced responsive documents to the warrant. It is undisputed that Agent Sampson reviewed the Microsoft data prior to the July deadline. (Mot. 1, at 6–7; Mot. 1 Ex. E; Sampson Decl. Ex. A.) While Defendant avers Agent Sampson searched the Microsoft data on August 3, 2015, and again on August 26, 2019, the evidence he cites to support his position is inapposite. (Mot. 1, at 6–7.) First, Defendant offers a printout of Microsoft's March 19, 2015, transmission with a date stamp of August 3, 2015. (Mot. 1 Ex. C.) This does not support Defendant's supposition that Agent Sampson reviewed any Microsoft data on this day—only that someone in possession of the transmittal email accessed the email on August 3, 2015. And, as the Court has already found, the March 19 email is not plausibly responsive to the warrant. Second, Defendant offers a declaration made by his forensic expert that states that the Microsoft data "was utilized in some manner on the case agent's hard drive on August 26, 2019 . . . ." (Gibson Decl. ¶ 10.) This statement does not support the assertion that Agent Sampson, or any agent, reviewed the Microsoft data after July 21, 2015—only that someone at HSI accessed the dataset "in some manner." (*Id.*)

Finally, Defendant argues agents at HSI reviewed the Microsoft data prior to receipt of the 2020 warrant. (Mot. 1, at 7–8.) Again, Defendant makes unsupported assumptions. He avers that an agent at HSI "necessarily reviewed, in a forensic software program, the underlying data that Microsoft produced" in 2015 to determine Agent

---

[2] Because the Government provides conflicting evidence as to when Microsoft produced the email data, the Court again does not take a position as to whether the production occurred on May 21 or 22, 2015.

Sampson had not finished her review of the Microsoft data. (*Id.* at 8.) However, nothing in the cited evidence suggests that anyone at HSI, including Agent Baker and HSI Supervisory Special Agent Oladele Salaam, viewed the Microsoft data rather than "bookmarks" made in a document review database to determine the status of the review, as Agent Baker attested to in his affidavit. (Mot. 1 Ex. D, at USAO_000361–62.)

All of Defendant's arguments regarding the 2015 warrant and the subsequent search of the Microsoft data thereafter are unavailing. For all of the reasons stated herein, Defendant's first motion is denied as to any alleged deficiencies with the 2015 warrant or the searches of the Microsoft data thereafter.[3]

B. 2020 Warrant

Defendant argues the evidence obtained following issuance of the June 2020 warrant should be suppressed for two reasons: (1) the warrant was not supported by probable cause, and (2) the warrant lacked particularity. (Mot. 1, at 20–24.)

1. Probable Cause

Probable cause exists when, under the totality of the circumstances set forth in a warrant affidavit, "there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). A "judge's finding of probable cause is entitled to great deference." *United States v. Clark*, 31 F.3d 831, 834 (9th Cir. 1994). A judge's decision to issue a search warrant must be upheld if the judge had a "substantial basis for concluding that the affidavit in support of the warrant established probable cause." *United States v. Greany*, 929 F.2d 523, 524 (9th Cir. 1991). "In borderline cases, preference will be accorded to warrants and to the decision of the magistrate issuing it." *United States v. Crews*, 502 F.3d 1130, 1135 (9th

---

[3] In his status report, Defendant represents that he sent discovery requests to the Government regarding the date HSI received the Microsoft data and asks that, if the Government's responses do not resolve this issue, the Court hold an evidentiary hearing. (Def. Status Report 3.) For the same reasons the Court denies Defendant's first motion as to the 2015 warrant, the Court denies his request for an evidentiary hearing.

Cir. 2007) (cleaned up).

In Agent Baker's affidavit filed in support of the 2020 application for a search warrant, he explained Agent Sampson's 2015 review of the CyberTip report as well as the email and suspected child pornography image, stated that Agent Sampson obtained a 2015 search warrant to review the Microsoft data, explained that he reviewed a database showing bookmarked items from the Microsoft data and determined Agent Sampson had not completed her review of the suspected child pornography images, and explained that the Microsoft data was still intact without tampering. (Mot. 1 Ex. D, at USAO_000355–68.) Magistrate Judge Maria A. Audero issued a search warrant permitting Agent Baker to review the Microsoft data, without a date limitation, as well as data on the physical devices. (*Id*. at USAO_000344–53.) Reviewing the materials available to Judge Audero at the time she issued the search warrant the Court finds there was sufficient probable cause for her decision to issue it. Judge Audero knew from Agent Baker's affidavit, among other things, that Microsoft had identified the image generating the NCMEC report as child pornography, that Agent Sampson had previously applied for and received a warrant to search Defendant's digital devices and the Microsoft data for child pornography, and that Agent Sampson had begun but not completed a review of images containing suspected child pornography. (Mot. 1 Ex. D.) The Court finds her decision to issue the 2020 warrant had a "substantial basis" for concluding Agent Baker's affidavit established probable cause. *See Greany*, 929 F.2d at 524.

Defendant's motion to suppress evidence for lack of probable cause is denied on this basis.[4]

---

[4] Defendant, in a footnote, argues that the 2020 warrant is invalid pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), because Agent Baker omitted key facts in his affidavit. (Mot. 1, at 24 n.3.) Specifically, Defendant argues that Agent Baker omitted any mention that the 2015 warrant included a specific date range and that the Government seized and retained all of the Microsoft data, some of which predated the date range in

2. Specificity

The Fourth Amendment requires that a warrant be specific. *United States v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993). "Specificity has two aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." *Id.* (internal quotation marks omitted).

Defendant avers the 2020 warrant was deficient because it was overbroad and insufficiently particular, authorizing the Government to search of all of Defendant's Microsoft data without any temporal restriction. (Mot. 1, at 22–24.) The Court disagrees. The 2020 warrant states what was sought, "evidence, contraband, fruits, or instrumentalities of" receipt, distribution, or possession of child pornography. (Mot. 1 Ex. D, at USAO_000370.) The warrant also lists 18 subcategories of information that could be seized. (*Id.* at USAO_000371–72.) The 2020 warrant does not contain a date range. (*See generally* Mot. 1 Ex. D.)

Defendant does not challenge the adequacy of the warrant's description of the items to be searched and seized. (*See* Mot. 1, at 22–24.) Instead, Defendant argues the 2020 warrant lacked particularity and was overbroad because it permitted a search of "all the data" in Defendant's Microsoft email, which was impermissible because "the

---

the 2015 warrant. (*Id.*) The Court disagrees that the 2020 warrant is invalid on this basis. Under *Franks*, a warrant is invalid if: (1) the affiant made false or misleading statements or omitted key facts; (2) the affiant made those false statements or omissions "intentionally" or "with reckless disregard for the truth"; and (3) without those statements or omissions, the affidavit would not establish probable cause. 438 U.S. at 155–56. Even if the Court were to find Agent Baker's purported omissions satisfied the first and second element of *Franks*, Defendant's challenge fails on the third prong. The Court already found that there was sufficient probable cause established in Agent Baker's 2020 affidavit, relied on by Judge Audero in issuing the 2020 warrant, without mention of the date range in the 2015 warrant. Defendant's footnote request for a *Franks* hearing is denied.

government ha[d] knowledge of the dates of suspected criminal activity . . . but ch[ose] not to include temporal restrictions for the search of electronic data." (Mot. 1, at 22.)

In support of his argument, Defendant cites four cases, none of which supports his position that the 2020 warrant was overbroad or insufficiently particular. In *United States v. Jolly*, this Court found a warrant was insufficiently particular because the government had knowledge of the date of suspected criminal activity but chose not to include a temporal restriction for the electronic data in the application for the warrant. Order Re: Pretrial Mots. at 4–7, *United States v. Jolly*, No. 2:20-cr-00438-MCS-1 (C.D. Cal. Mar. 4, 2022), ECF No. 248. However, in *Jolly*, the defendant was charged with possession with intent to distribute drugs on two specific dates. Indictment at 2–3, *United States v. Jolly*, No. 2:20-cr-00438-MCS-1 (C.D. Cal. Sept. 29, 2020), ECF No. 1. There, the government knew the dates on which the purported offenses occurred and, thus, the government's failure to limit the date range in the warrant application to the time around those two dates rendered the warrant insufficiently particular. Order Re: Pretrial Mots., *supra*, at 5–6; *see also United States v. Roberts*, 430 F. Supp. 3d 693, 716–18 (D. Nev. 2019) (finding the warrant at issue was overbroad because it permitted a search extending multiple days beyond a single act of suspected criminal activity); *United States v. Wey*, 256 F. Supp. 3d 355, 385 (S.D.N.Y. 2017) (finding a warrant lacking a timeframe was insufficiently particular where the affidavits filed in support of the warrant and the indictment identified "rather precise timeframes" the suspected criminal activity occurred); *United States v. Lofstead*, 574 F. Supp. 3d 831, 843 (D. Nev. 2021) (finding no justification for a warrant without a date restriction where the government had "very precise knowledge of the date and time texts and internet searches could be targeted" to uncover evidence of suspected criminal activity).

Unlike the cases Defendant cites, the suspected criminal activity here does not involve one select date or dates on which the suspected offense occurred. At the time Agent Baker applied for the 2020 warrant, the Government knew that Defendant likely possessed over 2,200 images of child abuse material or child exploitive material

possibly spanning over the 14 years Defendant had his Microsoft email. (Mot. 1 Ex. D, at USAO_000361–62.) Although the Government knew from the NCMEC report, and Agent Sampson's review thereof, that at least one of those images was from October 17, 2014, there was no way for the Government to know all the dates Defendant possessed, received, or transmitted the remaining images at the time Agent Baker applied for the 2020 warrant. (Mot. 2 Ex. B (providing details of the image that generated the NCMEC report, but no details of the other images produced in the Microsoft data)); *see Lofstead*, 574 F. Supp. 3d at 843 ("Temporal restrictions are not a de facto requirement, but courts that have allowed warrants without temporal limitations have reasoned the limitation would have served no limiting purpose."); *United States v. Sam*, No. CR19-0115-JCC, 2020 WL 2131285, at *3 (W.D. Wash. May 5, 2020) (finding a temporal limitation on a warrant would impede collection of pertinent evidence).

The 2020 warrant clearly listed the information sought and 18 specific subcategories of information that could be seized. (Mot. 1 Ex. D, at USAO_000370–72.) A temporal restriction on the 2020 warrant would have served no purpose given that there was a built-in start date (when Defendant first obtained an account with Microsoft) and end date (when Microsoft produced the email data), and given that the nature of Defendant's suspected criminal activity could have spanned that entire period.

Defendant's motion to suppress evidence obtained pursuant to the 2020 warrant for the warrant's lack of specificity is denied.

3. Delay

Defendant argues suppression of all evidence obtained in 2020 "is warranted because of the government's unreasonable delay between seizure of the Microsoft data and the digital devices in 2015 and obtaining the 2020 warrant." (Mot. 1, at 24.) Defendant's digital devices were forfeited to U.S. Customs and Broder Protection in January 2016. (Opp'n 8–9; Reply 1, at 9 n.4.) When property is forfeited to the United States, the United States becomes the owner of that property. *See United States v. Grp.*

of Islands Known as "Cayos De Barca," 185 F. Supp. 2d 117, 122 (D.P.R. 2001) (holding the government became proprietor over property immediately following its forfeiture). Therefore, Defendant did not own the digital devices after 2016. He cannot now challenge any purported constitutional violation related to the Government's search or seizure of them. *United States v. Baker*, 58 F.4th 1109, 1116 (9th Cir. 2023) (to assert a Fourth Amendment violation, the challenging party must have a possessory interest in the property seized). Accordingly, Defendant's argument pertaining to the Government's search and seizure of the digital devices in 2020 fails as a matter of law.

Defendant proffers, and the Government does not deny, that Defendant has a possessory interest in the email data. (Mot. 1, at 25–27.) However, Defendant does not cite a single case from this circuit that supports his argument that the Government's retention of his email data throughout the course of its investigation constitutes an unreasonable delay, thus warranting exclusion of evidence derived from that data. Moreover, the cases Defendant cites are distinguishable in that they do not discuss the government's search of email data produced by a private party to the government pursuant to a warrant. (*Id.*) In instances like these, where a defendant voluntarily shares his information with another—here with, Microsoft—the defendant has a diminished possessory interest in the information. *United States v. Wilkins*, 538 F. Supp. 3d 49, 92 (D.D.C. 2021). Defendant's interest, even his diminished one, must be weighed against the Government's interest in maintaining the Microsoft data. *United States v. Laist*, 702 F.3d 608, 616 (11th Cir. 2012). Here, the Government maintained the Microsoft data for purposes of conducting its investigation into Defendant's possession, receipt, and distribution of child pornography. (Opp'n 32.) That there was a pause in the investigation that resumed once a new agent was assigned Defendant's case is of no constitutional significance. The Government's interest in maintaining the data outweighs Defendant's diminished possessory interest in the email data. The Court denies Defendant's motion to suppress the email data on the basis that there was a temporal gap between the Government's seizure of the Microsoft data in 2015 and

Agent Baker's review of the data in 2020.

IV. CONCLUSION

Defendant's motions are denied.

IT IS SO ORDERED.

Dated: April 9, 2024

MARK C. SCARSI
UNITED STATES DISTRICT JUDGE